VEILLE TECHNOLOGIQUE

L'Architecture Zero Trust : Sécurité et Identité

SOMMAIRE

1. INTRODUCTION ET ÉTAT DES LIEUX

1.1 Objectif de la veille technologique

La veille technologique est un pilier de la formation BTS SIO. Elle consiste à observer l'environnement informatique pour anticiper les menaces et identifier les solutions de

demain. Aujourd'hui, les attaques se professionnalisent et visent particulièrement les prestataires de services informatiques qui gèrent des données étatiques.

J'ai choisi d'étudier le modèle **Zero Trust**. Ce concept change radicalement la protection d'un réseau : on ne fait plus confiance au réseau interne par défaut. L'objectif est de sécuriser chaque accès applicatif de manière individuelle.

1.2 La fin du modèle "Château Fort"

Pendant des années, la sécurité reposait sur le périmètre : un pare-feu solide protégeait un réseau local interne où tout le monde était considéré comme "sûr". Avec le Cloud et le télétravail, ce modèle est devenu obsolète. Un pirate qui vole un accès VPN aujourd'hui peut naviguer librement sur tous les serveurs internes.

Critère	Ancien modèle (VPN)	Modèle Zero Trust
Accès réseau	Segment complet (L3).	Application uniquement (L7).
Confiance	Vérifiée une fois à l'entrée.	Revérifiée à chaque requête.

2. PROBLÉMATIQUE ENTREPRISE (SOPRA STERIA & CHORUS PRO)

2.1 Le contexte Chorus Pro

Chez **Sopra Steria**, je travaille au support de **Chorus Pro**, le portail de facturation de

l'État. Cette plateforme manipule des données ultra-sensibles : RIB de fournisseurs, identités d'entreprises et montants financiers importants. La moindre fuite de données aurait un impact national.

2.2 Analyse des vecteurs de risque

Le tableau suivant détaille les risques de sécurité majeurs identifiés dans mon environnement de travail quotidien au Helpdesk :

Qui accède ?	Données manipulées	Risque critique
Technicien Support	Logs, comptes admin, RIB.	Vol du compte administrateur.
Flux EDI / API	Jetons d'authentification.	Injection de données financières.

2.3 Ma problématique de veille

"Comment l'architecture Zero Trust permet-elle à Sopra Steria de sécuriser l'accès à des données étatiques ultra-sensibles, tout en palliant les failles des réseaux traditionnels ?"

3. LE CONCEPT TECHNIQUE ZERO TRUST

3.1 "Never Trust, Always Verify"

Le principe est de considérer que n'importe quel ordinateur ou smartphone est potentiellement dangereux. Même branché dans les locaux de l'entreprise, un poste est considéré comme "étranger". Chaque demande d'accès doit être prouvée par l'identité (MFA), l'état du PC et la cohérence de l'heure et du lieu.

3.2 La Micro-segmentation

C'est une technique majeure qui consiste à découper le réseau en plein de petits morceaux isolés (des bulles de sécurité). Si un pirate réussit à entrer sur un serveur, il ne peut pas rebondir vers la base de données de Chorus Pro. La communication entre serveurs est interdite par défaut, ce qui arrête les virus.

3.3 L'inspection au niveau de l'application

Contrairement aux anciens systèmes, le Zero Trust analyse ce qu'il se passe à l'intérieur de la connexion (Couche 7). Si un technicien autorisé essaie tout à coup de télécharger des milliers de RIB en une minute, le système détecte cette anomalie et bloque l'accès immédiatement avant que la fuite ne soit complète.

4. LES 5 PILIERS DU MODÈLE DE MATURITÉ CISA

L'agence gouvernementale CISA a modélisé l'évolution vers le Zero Trust à travers 5 piliers fondamentaux. Une organisation doit faire évoluer chacun de ces axes pour

atteindre une sécurité optimale.

Détail technique des piliers :

- **L'Identité :** Utilisation obligatoire du MFA (Multi-Facteur) et de l'analyse comportementale.
- **Le Terminal (Device) :** Vérifier en temps réel que l'ordinateur est protégé par un antivirus à jour.
- **Le Réseau :** Passer d'un réseau physique ouvert à un réseau segmenté par logiciel.
- **L'Application :** Accès granulaire par application au lieu d'un accès au segment réseau.
- **La Donnée :** Chiffrement systématique des informations sensibles.

5. MISE EN ŒUVRE : LE CONTRÔLE DE POSTURE

5.1 Vérifier la santé de l'ordinateur

C'est l'innovation majeure : même avec le bon mot de passe, un technicien support ne peut pas se connecter si son PC est infecté. Le système interroge le poste de travail avant chaque ouverture de session vers Chorus Pro.

Composant vérifié	Prérequis technique	Action si échec
Antivirus / EDR	Agent actif et mis à jour il y a < 24h.	**Refus d'accès**
Certificat Machine	Certificat délivré par Sopra Steria présent.	**Refus d'accès**

Composant vérifié	Prérequis technique	Action si échec
Mises à jour OS	Correctifs de sécurité Windows installés.	**Quarantaine**

5.2 La réévaluation continue

La vérification n'est pas faite qu'une seule fois. Si mon antivirus se désactive pendant que je travaille sur Chorus Pro, le système coupe la connexion instantanément. Cela empêche qu'une menace ne s'active après la connexion de l'utilisateur.

6. L'ARCHITECTURE SDP (SOFTWARE DEFINED PERIMETER)

6.1 Le concept de "Black Cloud"

Le SDP est l'une des méthodes les plus sécurisées. Son principe est de rendre l'infrastructure de Chorus Pro totalement invisible sur Internet. Un pirate qui scannera le réseau ne verra aucun port ouvert. Le serveur est masqué tant que l'utilisateur n'a pas été authentifié par un contrôleur central.

6.2 Séparation du contrôle et des données

L'architecture repose sur deux couches bien distinctes pour plus de sécurité :

- **Le Plan de Contrôle :** Il valide l'identité et l'ordinateur *avant* toute connexion

réseau.

- **Le Plan de Données :** Une fois autorisé, un tunnel chiffré unique est créé vers l'application.

6.3 Protection contre les attaques massives

En rendant les serveurs invisibles, le SDP protège contre les attaques par déni de service (DDoS). Comme il n'y a pas de point d'entrée public visible, le pirate n'a pas de cible à attaquer. C'est une protection très forte pour les plateformes d'État.

7. COMPARATIF ET ANALYSE DES RISQUES

Solution	Point fort technique	Note
Zscaler (Private Access)	Rend les serveurs invisibles sur Internet. Très facile à déployer à grande échelle.	**5/5**
Cloudflare (Zero Trust)	Connexion ultra-rapide et protection DDoS. Idéal pour les accès web.	**5/5**
Okta Identity Engine	Gestion parfaite de l'identité et du MFA.	**4,5/5**

Solution	Point fort technique	Note
	S'intègre avec tout.	

7.1 Efficacité réelle face aux menaces

Menace identifiée	Risque sous VPN	Risque sous Zero Trust
Ransomware latéral	**Critique**	**Faible**
Vol de session admin	**Élevé**	**Moyen**

8. LIMITES ET GESTION DU CHANGEMENT

8.1 Les freins identifiés

Le passage au Zero Trust est un projet ambitieux qui rencontre des obstacles lors de sa mise en œuvre :

Obstacle technique / humain	Mesure de remédiation
Applications héritées (Legacy)	Utilisation de proxys d'identité pour ajouter du MFA.
Friction Utilisateur	Déploiement du SSO (Single Sign-On).
Dépendance au Cloud	Architecture de secours hybride locale.

8.2 Impact sur le Support technique

Le déploiement modifie le travail quotidien du Helpdesk. Au début, on remarque une hausse des tickets car des techniciens sont bloqués par un PC non conforme. Une formation des équipes est indispensable pour diagnostiquer rapidement si le blocage vient de l'identité ou de l'état de l'ordinateur.

9. CONCLUSION GÉNÉRALE

L'architecture Zero Trust n'est plus une simple évolution technologique, c'est une réponse stratégique indispensable face à l'obsolescence des modèles de sécurité traditionnels. La dissolution du périmètre physique de l'entreprise impose de passer

d'une confiance automatique à une vérification continue.

Pour une organisation comme **Sopra Steria**, la sécurisation de plateformes critiques telles que **Chorus Pro** repose désormais sur quatre piliers d'efficacité :

- **La réduction de la surface d'attaque :** Le principe de vérification systématique élimine les accès inutiles.
- **Le confinement des menaces :** La micro-segmentation bloque radicalement le mouvement latéral des ransomwares.
- **Le contrôle de conformité :** La vérification stricte de la santé des terminaux garantit que seuls des postes sains accèdent aux données d'État.
- **La traçabilité totale :** Le modèle offre une visibilité parfaite sur chaque accès, facilitant les audits de sécurité.

Malgré les défis réels liés à la mise en place technique et au changement d'habitude des employés, le gain en sécurité est indiscutable. Le Zero Trust devient le socle nécessaire pour garantir la protection des données les plus sensibles de notre économie numérique.

10. ANNEXES

10.1 Méthodologie de Veille

- **Sourcing :** Utilisation de Feedly pour surveiller les flux RSS de l'ANSSI, de la

CISA et de blogs spécialisés en cybersécurité.

- **Alertes ciblées :** Paramétrage de Google Alerts sur les mots-clés stratégiques : "ZTNA", "Micro-segmentation", "Software Defined Perimeter".
- **Analyse documentaire :** Étude de la publication 800-207 du NIST et des livres blancs techniques des éditeurs (Cloudflare, Zscaler).

10.2 Glossaire Technique

- **ZTNA :** Technologie remplaçant le VPN en connectant l'utilisateur directement à une application après vérification.
- **Micro-segmentation :** Technique consistant à diviser le réseau en petites zones isolées pour bloquer les virus.
- **Posture Check :** Analyse de l'état de santé d'un ordinateur (antivirus, mises à jour) avant sa connexion.
- **SDP :** Périmètre défini par logiciel pour rendre l'infrastructure invisible.

10.3 Sources

NIST Publication 800-207, CISA Zero Trust Maturity Model 2.0, ANSSI Recommandations stratégiques, Blogs techniques Cloudflare et Zscaler.